

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-203371

(43) 公開日 平成11年(1999) 7月30日

(51) Int.Cl.⁶
G 0 6 F 19/00
G 0 6 K 17/00
19/10
G 0 7 D 9/00
G 0 7 F 7/08

識別記号

4 3 6

F I

G 0 6 F 15/30 3 6 0
G 0 6 K 17/00 T
G 0 7 D 9/00 4 3 6 Z
G 0 7 G 1/12 3 2 1 P
1/14

審査請求 未請求 請求項の数13 O L (全 15 頁) 最終頁に続く

(21) 出願番号 特願平10-2441

(22) 出願日 平成10年(1998) 1月8日

(71) 出願人 000152859

株式会社日本コンラックス
東京都千代田区内幸町2丁目2番2号

(72) 発明者 太田 通博

埼玉県坂戸市伊豆の山町55-2

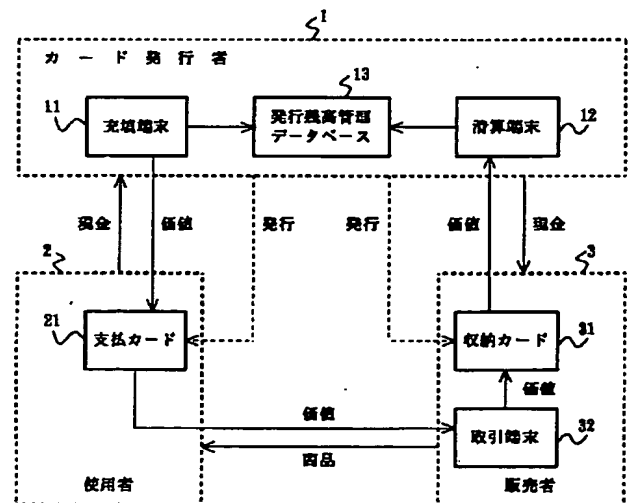
(74) 代理人 弁理士 木村 高久

(54) 【発明の名称】 ICカードを用いた決済方法およびシステム

(57) 【要約】

【課題】匿名性を維持しつつ、不正があった場合の発見を早くし、かつ追跡が可能で利便性が高く比較的簡易な構成で実現できるICカードを用いた決済方法およびシステムを提供する。

【解決手段】使用者(2)が身分を明かすことなく充填端末(11)から支払カード(21)への価値の充填を行い、販売者(3)との取引を行う際には、取引端末(32)を単なる伝送手段として支払カード(21)と収納カード(31)が相互認証を行って価値を移動させる。



【特許請求の範囲】

【請求項1】 商品若しくはサービスの対価となる価値情報を格納したＩＣカードを利用し、前記価値情報を移動させることにより決済を行うＩＣカードを用いた決済方法において、

前記対価の支払者が使用する第１のＩＣカードと該第１のＩＣカードに前記価値情報を充填する充填端末とが相互認証を行い、該相互認証が成功した場合に前記充填端末から前記第１のＩＣカードに前記価値情報の充填を行い、

前記対価の支払者と該対価の受領者とが決済を行う際に、前記第１のＩＣカードと前記受領者が使用する第２のＩＣカードとが相互認証を行い、該相互認証が成功した場合に前記第１のＩＣカードから前記第２のＩＣカードへ前記価値情報の移動を行い、

前記第２のＩＣカードと該第２のＩＣカードから前記価値情報を受領して清算を行う清算端末とが相互認証を行い、該相互認証が成功した場合に前記第２のＩＣカードから前記清算端末に前記価値情報を移動して清算を行うことを特徴とするＩＣカードを用いた決済方法。

【請求項2】 前記第２のＩＣカードは、前記受領者に固有の所有者識別符号を記憶し、前記清算端末へ前記価値情報を移動させる場合に、該価値情報の移動とともに前記所有者識別符号を通知することを特徴とする請求項1記載のＩＣカードを用いた決済方法。

【請求項3】 前記第１のＩＣカードは、該第１のＩＣカードに固有のカード識別符号を記憶し、前記充填端末は、前記価値情報の充填を行う場合に該価値情報の額と前記カード識別符号を対応させて発行残高管理データベースに記憶し、前記第２のＩＣカードは、前記第１のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領し、前記清算端末は、前記第２のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領するとともに、該受領した価値情報の額と該カード識別符号とを前記発行残高管理データベースに記憶し、前記発行残高管理データベースは、前記カード識別符号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする請求項1または2記載のＩＣカードを用いた決済方法。

【請求項4】 前記充填端末は、前記価値情報の充填を行う場合に該価値情報に固有の発行番号を付し、該価値情報の額と前記発行番号を対応させて発行残高管理データベースに記憶し、前記第２のＩＣカードは、前記第１のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領し、

前記清算端末は、前記第２のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領するとともに、該受領した価値情報の額と該発行番号とを前記発行残高管理データベースに記憶し、前記発行残高管理データベースは、前記発行番号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする請求項1または2記載のＩＣカードを用いた決済方法。

【請求項5】 前記相互認証は、

10 前記第１のＩＣカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第２のＩＣカードへ送信し、前記暗号化送信情報が前記第２のＩＣカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較確認することで、前記第２のＩＣカードを認証し、

前記第２のＩＣカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第１のＩＣカードへ送信し、前記暗号化送信情報が前記第１のＩＣカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較確認することで、前記第１のＩＣカードを認証することで行うことを特徴とする請求項1乃至4のいずれかに記載のＩＣカードを用いた決済方法。

30 【請求項6】 前記第１のＩＣカードと前記第２のＩＣカードとが、同一のＩＣカード内に構成されることを特徴とする請求項1乃至5のいずれかに記載のＩＣカードを用いた決済方法。

【請求項7】 商品若しくはサービスの対価となる価値情報を格納したＩＣカードを利用し、前記価値情報を移動させることにより決済を行うＩＣカードを用いた決済システムにおいて、

前記対価の支払者が使用する第１のＩＣカードと、
40 前記対価の受領者が使用する第２のＩＣカードと、
前記第１のＩＣカードに前記価値情報を充填する充填端末と、
前記第２のＩＣカードから前記価値情報を受領して清算を行う清算端末と、
前記第１のＩＣカードと前記第２のＩＣカードとの間の通信を仲介する取引端末と、
前記充填端末が充填した価値情報の額と前記清算端末が清算した価値情報の額とを記憶管理する発行残高管理データベースとを具備し、

50 前記第１のＩＣカードは、前記充填端末と前記第２のＩ

3

Cカードとのいずれかとの間で相互認証を行う第1の相互認証手段と、前記価値情報を格納する第1の価値情報格納手段と、該第1の価値情報格納手段に格納された前記価値情報を移動させる第1の価値情報移動手段とを具備し、

前記第2のICカードは、前記清算端末と前記第1のICカードとのいずれかとの間で相互認証を行う第2の相互認証手段と、前記価値情報を格納する第2の価値情報格納手段と、該第2の価値情報格納手段に格納された前記価値情報を移動させる第2の価値情報移動手段とを具備し、

前記充填端末は、前記第1のICカードとの間で相互認証を行う第3の相互認証手段と、前記価値情報を充填する価値情報充填手段と、該価値情報充填手段が充填した価値情報の額を前記発行残高管理データベースに記憶させる充填額記憶手段とを具備し、

前記清算端末は、前記第2のICカードとの間で相互認証を行う第4の相互認証手段と、前記価値情報を受領して清算する価値情報清算手段と、該価値情報清算手段により清算された価値情報の額を前記発行残高管理データベースに記憶させる清算額記憶手段とを具備し、

前記取引端末は、前記第1のICカードに決済取引の開始を通知する取引開始通知手段と、前記第1のICカードと前記第2のICカードとの間の通信を仲介する伝送手段とを具備することを特徴とするICカードを用いた決済システム。

【請求項8】 前記第2のICカードは、前記受領者に固有の所有者識別符号を記憶する所有者識別符号格納手段と、

前記清算端末との間で清算を行う場合に、前記第2の価値情報移動手段による価値情報の移動とともに前記所有者識別符号を前記清算端末に通知する所有者識別符号通知手段とをさらに具備することを特徴とする請求項7記載のICカードを用いた決済システム。

【請求項9】 前記第1の価値情報移動手段は、前記第1の価値情報格納手段に格納される価値情報の加減算を行う第1の価値情報加減算手段を具備し、前記充填端末から価値情報の充填を受けるときは前記第1の価値情報加減算手段が前記第1の価値情報格納手段に格納されている価値情報に充填額を加算し、前記第2のICカードへの価値情報の支払を行う場合には前記第1の価値情報加減算手段が前記第1の価値情報格納手段に格納されている価値情報から支払額を減算し、

前記第2の価値情報移動手段は、前記第2の価値情報格納手段に格納される価値情報の加減算を行う第2の価値情報加減算手段を具備し、前記第1のICカードから価値情報を受領するときには前記第2の価値情報加減算手段が前記第2の価値情報格納手段に格納されている価値情報に受領額を加算し、前記清算端末との間で清算を行う場合には前記第2の価値情報加減

4

算手段が前記第2の価値情報格納手段に格納されている価値情報から清算額を減算することを特徴とする請求項7記載のICカードを用いた決済システム。

【請求項10】 前記第1のICカードは、該第1のICカードに固有のカード識別符号を格納するカード識別符号格納手段と、前記充填端末から価値情報の充填を受ける場合に前記カード識別符号を該充填端末に通知するカード識別符号通知手段とをさらに具備し、前記充填額記憶手段は、前記価値情報充填手段が前記第1のICカードに充填する価値情報の額と前記カード識別符号通知手段により通知されたカード識別符号とを対応させて前記発行残高管理データベースへ記憶し、前記第1の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、

前記第2の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、

前記第2の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記カード識別符号とを対応させて格納し、

前記清算額記憶手段は、前記清算額記憶手段が前記第2のICカードとの間で清算する価値情報の額と前記カード識別符号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする請求項7または8記載のICカードを用いた決済システム。

【請求項11】 前記価値情報充填手段は、前記価値情報の充填を行う場合に該価値情報に固有の発行番号を生成する発行番号生成手段をさらに具備し、

前記充填額記憶手段は、前記価値情報充填手段が前記第1のICカードに充填する価値情報の額と前記発行番号生成手段により生成された発行番号とを対応させて前記発行残高管理データベースへ記憶し、

前記第1の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、

前記第1の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、

前記第2の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、

前記第2の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、

前記清算額記憶手段は、前記清算額記憶手段が前記第2のICカードとの間で清算する価値情報の額と前記発行番号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする請求項7または8記載のICカードを用いた決済システム。

【請求項12】 前記第1の相互認証手段と前記第2の相互認証手段と前記第3の相互認証手段と前記第4の相互認証手段とは、

任意の乱数を発生させる乱数発生手段と、該乱数発生手段が発生した乱数と所定の情報とを合成する合成手段

と、該合成手段の出力を暗号化する暗号化手段と、暗号化された受信情報を復号化する復号化手段と、該復号化手段により復号化された情報を所定の情報と乱数とに分離する分離手段をさらに具備し、

前記乱数発生手段が発生した乱数を前記合成手段で所定の情報と合成して前記暗号化手段で暗号化して送信するとともに、

該送信先で復号化および分離された前記乱数が前記所定の情報に対する返信情報に合成されて暗号化されたことを、該暗号化された返信情報を前記復号化手段で復号化して前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とを前記比較手段で比較し、

該比較の結果、前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とが同一であった場合に前記送信先が同一の暗号鍵を有する正当な通信相手であると認証することを特徴とする請求項7乃至11のいずれかに記載のICカードを用いた決済システム。

【請求項13】 前記第1のICカードと前記第2のICカードとが、

同一のICカード内に構成されることを特徴とする請求項7乃至12のいずれかに記載のICカードを用いた決済システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ICカードを用いた決済方法およびシステムに関し、特に、比較的簡易な構成で、匿名性を維持し、不正の早期検出や価値の転々流通を行うことのできるICカードを用いた決済方法およびシステムに関する。

【0002】

【従来技術】ICカードを用いて決済を行う決済システムは、価値ベースの決済と信用ベースの決済とに分類できる。価値ベースの決済は、比較的に現金による決済に近く、ICカードに価値が充填されていて、その価値を移動することで決済するものである。信用ベースの決済は、クレジットカードを利用した決済システムに代表されるように、ICカードに記録された個人情報に基づいて承認行為を行い、オンライン口座資金移動によって決済するものである。

【0003】また、価値ベースの決済は、その価値の移動形態から現金型と前払型に分類することができる。

【0004】現金型では、現金での取引と同様に、取引により受け取った価値を別の取引の支払に利用することができる。このため、現金型には匿名性、つまり誰が何処でどの様な取引を行ったかは追跡されないが、価値が

転々流通するために偽造価値が混入された場合、それを発見することは困難である。

【0005】前払型では、価値の発行元がICカードに充填した価値は、一度取引された後に、必ず価値の発行元で清算する、つまり商品を購入した場合にはその価値は商品と引き替えに消滅（清算以外の使用不能）することになる。また、使用時に暗証番号を必要とすることが多い。このため、偽造価値の混入等の不正に対しては強固なシステムであるが、匿名性が無く、利便性にも欠けることになる。

【0006】このように、現金型と前払型には夫々長所と短所があるが、最近では現金型と前払型の長所を兼ね備えた決済システムも提案されている。

【0007】この決済システムは、匿名性を維持しつつも不正が行われた場合には、一定の追跡ができるシステムであり、例えば、ICカードの利用者の他に、登録機関と発行機関、金融機関で構成されるシステムである。

【0008】登録機関は、利用者が利用する公開鍵（秘密鍵と対をなして使用する暗号鍵であり、秘密鍵は利用者のみが知り得る暗号鍵）と利用者の名前を対にして登録しておき、この公開鍵の正当性を第三者に対して保証する。また、この公開鍵は登録機関のデジタル署名と併せて登録書としてICカードに格納される。

【0009】発行機関は、価値の発行と管理、不正の検出を行うが、利用者は発行機関に対して名前を明かさず、登録機関の保証の元に公開鍵を名前の代わり、つまり仮名として利用することでICカードへの価値の充填を行うことができるため匿名性を維持できる。

【0010】金融機関は利用者の口座を管理し、発行機関でのICカードへの価値の充填に必要な依頼書を利用者の要請に基づき発行するが、利用者の仮名（公開鍵）と実名が一致しないようにブラインド署名という技術を用いて、利用者の仮名が金融機関に知られることなく、依頼書を発行することができる。

【0011】ここで、発行機関が発行した価値の流通について説明する。図11は、流通過程でのICカード内に格納されている価値の形態を示した図である。

【0012】図11(a)は、発行機関が利用者A（仮名aaa）に対して発行した価値を示しており、価値1011には、その価値の額面1012（10000円）と識別番号1013（xxxxx：紙幣に付された紙幣番号のようなもの）、発行先の仮名1014（aaa）、発行機関のデジタル署名1015が付されている。

【0013】利用者Aがこの価値1011の全部または一部を利用者B（仮名bbb）へ対価として支払または譲渡する場合には、図11(b)に示すように価値1011に譲渡証を添付して支払または譲渡する。

【0014】図11(b)に示す譲渡証1021は、価値1011の他に譲渡する額面1022（4500円）

と譲渡証番号1023 (yyyyy)、譲渡先の仮名1024 (bbb)、利用者Aの署名1025 (aaa) が付されている。署名1025は、利用者Aのみが知っている(はず)の秘密鍵で価値1011と額面1022、譲渡証番号1023、仮名1024を暗号化することで行われており、利用者Bは公開されている公開鍵(仮名として利用されているaaa)で復号化することで検証できる。また、譲渡証番号1023は、同じ番号が生じないように受け取り側(利用者B)の責任で決定する。

【0015】利用者Aは、他の利用者への価値1011の譲渡等を行うこともできるが、譲渡した価値の額面の総和が額面1012(10000円)を越えることができないのはいうまでもない(利用者Aの所有するICカードの制御による)。

【0016】同様に、利用者Bが利用者C(仮名ccc)へ価値の譲渡等を行う場合には、図11(c)に示すように価値1011を含む譲渡証1021にさらに譲渡証1031を添付して譲渡等を行う。図11(c)に示す譲渡証1031は、譲渡証1021の他に譲渡する額面1032(2100円)と譲渡証番号1033 (zzzz)、譲渡先の仮名1034 (ccc)、利用者Bの署名1035 (bbb) が付されている。この署名1035も同様に利用者Bのみが知っている秘密鍵を利用して行われる。

【0017】このように価値1011は、任意の額面で分割して譲渡することができ、譲渡証の連鎖により転々と流通する。

【0018】ところで、この価値1011の流通の過程で不正が生じたとしても、最終的に発行機関での清算(価値の回収)の際に発見することができる。例えば、利用者Bが利用者Aから譲渡を受けた価値1011(譲渡証1021)をコピーして何度も利用したとする。この場合、利用者Bが利用できるのは譲渡先が自分に指定された譲渡証1021のみであり(価値1011を抽出してコピーしようとしても、発行先の指定がaaaであるので譲渡される側が受け取りを拒否する)、譲渡証1021は署名1025で暗号化されているため譲渡証番号1023を書き換えることができない。したがって、譲渡証1021をコピーしても同一の譲渡証番号が付されたままとなり、これらを使用すれば、発行機関で譲渡証番号に基づいて不正をおこなった人物が利用者Bであると特定される。発行機関は、利用者Bが不正を行ったことを特定できれば登録機関に問い合わせ、利用者Bの実名を取得して摘発することができる。

【0019】

【発明が解決しようとする課題】ところで、上述の現金型と前払型の長所を兼ね備えた決済システムでは、不正が行われた際に、この不正が発見されるまでに要する時間が長く、盗難カードに基づいて不正が行われた場合に

は、追跡がほぼ不可能となる。

【0020】また、利用者が使用する各ICカードでは多量のメモリと計算時間を必要とするためコストが高くなるといった問題点があった。

【0021】そこで、この発明は、匿名性を維持しつつ、不正があった場合の発見を早くし、かつ追跡が可能で利便性が高く比較的簡易な構成で実現できるICカードを用いた決済方法およびシステムを提供することを目的とする。

10 【0022】

【課題を解決するための手段】上述した目的を達成するため、請求項1の発明では、商品若しくはサービスの対価となる価値情報を格納したICカードを利用し、前記価値情報を移動させることにより決済を行うICカードを用いた決済方法において、前記対価の支払者が使用する第1のICカードと該第1のICカードに前記価値情報を充填する充填端末とが相互認証を行い、該相互認証が成功した場合に前記充填端末から前記第1のICカードに前記価値情報の充填を行い、前記対価の支払者と該対価の受領者とが決済を行う際に、前記第1のICカードと前記受領者が使用する第2のICカードとが相互認証を行い、該相互認証が成功した場合に前記第1のICカードから前記第2のICカードへ前記価値情報の移動を行い、前記第2のICカードと該第2のICカードから前記価値情報を受領して清算を行う清算端末とが相互認証を行い、該相互認証が成功した場合に前記第2のICカードから前記清算端末に前記価値情報を移動して清算を行うことを特徴とする。

30 【0023】また、請求項2の発明では、請求項1の発明において、前記第2のICカードは、前記受領者に固有の所有者識別符号を記憶し、前記清算端末へ前記価値情報を移動させる場合に、該価値情報の移動とともに前記所有者識別符号を通知することを特徴とする。

40 【0024】また、請求項3の発明では、請求項1または2の発明において、前記第1のICカードは、該第1のICカードに固有のカード識別符号を記憶し、前記充填端末は、前記価値情報の充填を行う場合に該価値情報の額と前記カード識別符号を対応させて発行残高管理データベースに記憶し、前記第2のICカードは、前記第1のICカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領し、前記清算端末は、前記第2のICカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領するとともに、該受領した価値情報の額と該カード識別符号とを前記発行残高管理データベースに記憶し、前記発行残高管理データベースは、前記カード識別符号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする。

50 【0025】また、請求項4の発明では、請求項1また

は2の発明において、前記充填端末は、前記価値情報の充填を行う場合に該価値情報に固有の発行番号を付し、該価値情報の額と前記発行番号を対応させて発行残高管理データベースに記憶し、前記第2のICカードは、前記第1のICカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領し、前記清算端末は、前記第2のICカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領するとともに、該受領した価値情報の額と該発行番号とを前記発行残高管理データベースに記憶し、前記発行残高管理データベースは、前記発行番号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする。

【0026】また、請求項5の発明では、請求項1乃至4のいずれかの発明において、前記相互認証は、前記第1のICカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第2のICカードへ送信し、前記暗号化送信情報が前記第2のICカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較することで確認することで、前記第2のICカードを認証し、前記第2のICカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第1のICカードへ送信し、前記暗号化送信情報が前記第1のICカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較確認することで、前記第1のICカードを認証することで行うことを特徴とする。

【0027】また、請求項6の発明では、請求項1乃至5のいずれかの発明において、前記第1のICカードと前記第2のICカードとが、同一のICカード内に構成されることを特徴とする。

【0028】また、請求項7の発明では、商品若しくはサービスの対価となる価値情報を格納したICカードを利用し、前記価値情報を移動させることにより決済を行うICカードを用いた決済システムにおいて、前記対価の支払者が使用する第1のICカードと、前記対価の受領者が使用する第2のICカードと、前記第1のICカードに前記価値情報を充填する充填端末と、前記第2のICカードから前記価値情報を受領して清算を行う清算端末と、前記第1のICカードと前記第2のICカードとの間の通信を仲介する取引端末と、前記充填端末が充填した価値情報の額と前記清算端末が清算した価値情報の額とを記憶管理する発行残高管理データベースとを具備し、前記第1のICカードは、前記充填端末と前記第

2のICカードとのいずれかとの間で相互認証を行う第1の相互認証手段と、前記価値情報を格納する第1の価値情報格納手段と、該第1の価値情報格納手段に格納された前記価値情報を移動させる第1の価値情報移動手段とを具備し、前記第2のICカードは、前記清算端末と前記第1のICカードとのいずれかとの間で相互認証を行う第2の相互認証手段と、前記価値情報を格納する第2の価値情報格納手段と、該第2の価値情報格納手段に格納された前記価値情報を移動させる第2の価値情報移動手段とを具備し、前記充填端末は、前記第1のICカードとの間で相互認証を行う第3の相互認証手段と、前記価値情報を充填する価値情報充填手段と、該価値情報充填手段が充填した価値情報の額を前記発行残高管理データベースに記憶させる充填額記憶手段とを具備し、前記清算端末は、前記第2のICカードとの間で相互認証を行う第4の相互認証手段と、前記価値情報を受領して清算する価値情報清算手段と、該価値情報清算手段により清算された価値情報の額を前記発行残高管理データベースに記憶させる清算額記憶手段とを具備し、前記取引端末は、前記第1のICカードに決済取引の開始を通知する取引開始通知手段と、前記第1のICカードと前記第2のICカードとの間の通信を仲介する伝送手段とを具備することを特徴とする。

【0029】また、請求項8の発明では、請求項7の発明において、前記第2のICカードは、前記受領者に固有の所有者識別符号を記憶する所有者識別符号格納手段と、前記清算端末との間で清算を行う場合に、前記第2の価値情報移動手段による価値情報の移動とともに前記所有者識別符号を前記清算端末に通知する所有者識別符号通知手段とをさらに具備することを特徴とする。

【0030】また、請求項9の発明では、請求項7の発明において、前記第1の価値情報移動手段は、前記第1の価値情報格納手段に格納される価値情報の加減算を行う第1の価値情報加減算手段を具備し、前記充填端末から価値情報の充填を受けるときは前記第1の価値情報加減算手段が前記第1の価値情報格納手段に格納されている価値情報に充填額を加算し、前記第2のICカードへの価値情報の支払を行う場合には前記第1の価値情報加減算手段が前記第1の価値情報格納手段に格納されている価値情報から支払額を減算し、前記第2の価値情報移動手段は、前記第2の価値情報格納手段に格納される価値情報の加減算を行う第2の価値情報加減算手段を具備し、前記第1のICカードから価値情報を受領するときには前記第2の価値情報加減算手段が前記第2の価値情報格納手段に格納されている価値情報に受領額を加算し、前記清算端末との間で清算を行う場合には前記第2の価値情報加減算手段が前記第2の価値情報格納手段に格納されている価値情報から清算額を減算することを特徴とする。

【0031】また、請求項10の発明では、請求項7ま

たは8の発明において、前記第1のICカードは、該第1のICカードに固有のカード識別符号を格納するカード識別符号格納手段と、前記充填端末から価値情報の充填を受ける場合に前記カード識別符号を該充填端末に通知するカード識別符号通知手段とをさらに具備し、前記充填額記憶手段は、前記価値情報充填手段が前記第1のICカードに充填する価値情報の額と前記カード識別符号通知手段により通知されたカード識別符号とを対応させて前記発行残高管理データベースへ記憶し、前記第1の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、前記第2の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、前記第2の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記カード識別符号とを対応させて格納し、前記清算額記憶手段は、前記清算額記憶手段が前記第2のICカードとの間で清算する価値情報の額と前記カード識別符号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする。

【0032】また、請求項11の発明では、請求項7または8の発明において、前記価値情報充填手段は、前記価値情報の充填を行う場合に該価値情報に固有の発行番号を生成する発行番号生成手段をさらに具備し、前記充填額記憶手段は、前記価値情報充填手段が前記第1のICカードに充填する価値情報の額と前記発行番号生成手段により生成された発行番号とを対応させて前記発行残高管理データベースへ記憶し、前記第1の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、前記第1の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、前記第2の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、前記第2の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、前記清算額記憶手段は、前記清算額記憶手段が前記第2のICカードとの間で清算する価値情報の額と前記発行番号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする。

【0033】また、請求項12の発明では、請求項7乃至11のいずれかの発明において、前記第1の相互認証手段と前記第2の相互認証手段と前記第3の相互認証手段と前記第4の相互認証手段とは、任意の乱数を発生させる乱数発生手段と、該乱数発生手段が発生した乱数と所定の情報とを合成する合成手段と、該合成手段の出力を暗号化する暗号化手段と、暗号化された受信情報を復号化する復号化手段と、該復号化手段により復号化された情報を所定の情報と乱数とに分離する分離手段をさらに具備し、前記乱数発生手段が発生した乱数を前記合成

手段で所定の情報と合成して前記暗号化手段で暗号化して送信するとともに、該送信先で復号化および分離された前記乱数が前記所定の情報に対する返信情報に合成されて暗号化されたことを、該暗号化された返信情報を前記復号化手段で復号化して前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とを前記比較手段と比較し、該比較の結果、前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とが同一であった場合に前記送信先が同一の暗号鍵を有する正当な通信相手であると認証することを特徴とする。

【0034】また、請求項13の発明では、請求項7乃至12のいずれかの発明において、前記第1のICカードと前記第2のICカードとが、同一のICカード内に構成されることを特徴とする。

【0035】

【発明の実施の形態】以下、この発明に係わるICカードを用いた決済方法およびシステムの一実施例を添付図面を参照して詳細に説明する。

【0036】図1は、決済システムのシステム構成を示すブロック図である。決済システムは、カード発行者1が有する充填端末11と清算端末12と発行残高管理データベース13、使用者2が有する支払カード21、販売者3が有する収納カード31と取引端末32で構成される。

【0037】充填端末11は、支払カード21に商品やサービス等の対価となる価値を充填し、清算端末12は収納カード31から価値を回収する。発行残高管理データベース13は、発行済みで未回収の残高を記憶するデータベースである。

【0038】使用者2が販売者3から商品やサービス等の提供を受け、その対価として価値を支払う際には、取引端末32を介して支払カード21から収納カード31へ価値の移動を行う。

【0039】図2は、充填端末11の詳細を示すブロック図である。充填端末11は、相互認証手段111、価値充填手段112、送／受信手段113、発行残高管理手段114を具備して構成される。相互認証手段111は、送／受信手段113を介して接続される支払カード21とその正当性を相互に認証する手段であり、価値充填手段112は相互認証手段111により支払カード21が認証された場合に支払カード21に価値を充填する。発行残高管理手段114は、発行残高管理データベース13に記憶されている価値の発行残高の参照や更新を行う。

【0040】図3は、清算端末12の詳細を示すブロック図である。清算端末12は、相互認証手段121、価値格納手段122、送／受信手段123、発行残高管理手段124を具備して構成される。相互認証手段121は、送／受信手段123を介して接続される収納カード31とその正当性を相互に認証する手段であり、価値格

納手段122は相互認証手段121により収納カード31が認証された場合に収納カード31から価値を受領して格納する。発行残高管理手段124は、発行残高管理データベース13に記憶されている価値の発行残高の参照や更新を行う。

【0041】図4は、支払カード21の詳細を示すブロック図である。支払カード21は、相互認証手段211、価値加減算手段212、価値格納手段213、送/受信手段214、カードID格納手段215を具備して構成される。相互認証手段211は、送/受信手段214を介して接続される充填端末11や収納カード31とその正当性を相互に認証する手段であり、価値加減算手段212は、相互認証手段211により充填端末11が認証されれば充填端末11から充填される価値を価値格納手段213に格納されている価値に加算し、収納カード31が認証されれば、価値格納手段213に格納されている価値をその取引額に応じて減算する。また、カードID格納手段215は、支払カード21に固有のカードID番号を格納する手段であり、このカードID番号により発行者1は発行済みの価値の管理を行う。

【0042】図5は、収納カード31の詳細を示すブロック図である。収納カード31は、相互認証手段311、価値加減算手段312、価値格納手段313、送/受信手段314、所有者ID格納手段315を具備して構成される。相互認証手段311は、送/受信手段314を介して接続される清算端末12や支払カード21とその正当性を相互に認証する手段であり、価値加減算手段312は、相互認証手段311により清算端末12が認証されればから価値格納手段313に格納されている価値を減算して清算端末12へ渡し、支払カード21が認証されれば、支払カード21から取引額に応じた価値を受領して価値格納手段313に格納されている価値に加算する。また、所有者ID格納手段315は、収納カード31の所有者に固有の所有者ID番号を格納する手段である。

【0043】図6は、取引端末32の詳細を示すブロック図である。取引端末32は、支払カード21と接続される送/受信手段321と収納カード31と接続される送/受信手段322と支払カード21に取引の開始を通知する取引介し通知手段323を具備して構成される。取引端末32は、取引開始通知手段323が発生する取引開始要求を除いて送/受信手段321と送/受信手段322が送受するデータには介入しない。

【0044】ここで、図7を参照して、価値の充填、取引、清算の際の充填端末11、清算端末12、支払カード21、収納カード31、取引端末32の動作および通信データの流れを説明する。

【0045】図7は、価値の充填、取引、清算の際の各々の通信データの流れを示した図である。

【0046】図7(a)は、価値充填の際に支払カード

21と充填端末11との間で授受されるデータの流れを示した図である。

【0047】まず、支払カード21が充填端末11に挿入され、支払カード21の送/受信手段214と充填端末11の送/受信手段113が接続されて支払カード21と充填端末11が通信可能な状態になると、支払カード21が充填要求を充填端末11に送信する(ステップ501)。このとき、充填要求は支払カード21の相互認証手段211で数0と合成されて暗号化され、さらに該相互認証手段211が発生した乱数R1とステータスS1が付加されて送信される。

【0048】充填要求を受信した充填端末11は、この充填端末11の相互認証手段111で乱数R1とステータスS1を分離した後、復号化および数0との分離を行うことで充填要求を受信する。次に、充填端末11は支払カード21に該支払カードのカードIDを通知することを要求するが、このとき、前記相互認証手段111が先に分離した乱数R1とID通知要求を合成して暗号化し、この暗号化情報にさらに前記相互認証手段111が発生した乱数R2とステータスS2を合成した合成情報を支払カード21に送信する(ステップ502)。

【0049】合成情報を受信した支払カード21は、この支払カード21の相互認証手段211で受信した合成情報から乱数R2とステータスS2を分離して暗号化情報を取得し、この暗号化情報を復号化してID通知要求と乱数R1とに分離する。ここで、前記相互認証手段211は、分離した乱数R1と先に発生した乱数R1を比較し、両者が一致すれば充填端末11が正当な処理(乱数R1の分離と合成および暗号化)を行った、つまり充填端末11が支払カード21と共通の暗号鍵を有する正当な充填端末であると認証し、受信したID通知要求に対する処理を行う。

【0050】支払カード21は、受信したID通知要求に対して、支払カード21のカードID格納手段215に格納されているカードIDを支払カード21の相互認証手段211で分離した乱数R2と合成して暗号化し、さらに前記相互認証手段211が発生した乱数R3とステータスS3を合成した合成情報として充填端末11に送信する(ステップ503)。

【0051】合成情報を受信した充填端末11は、充填端末11の相互認証手段111で受信した合成情報から乱数R3とステータスS3を分離して暗号化情報を取得し、この暗号化情報を復号化してカードIDと乱数R2とに分離する。前記相互認証手段111は、分離した乱数R2と先に発生した乱数R2を比較し、両者が一致すれば支払カード21が正当な処理(乱数R2の分離と合成および暗号化)を行った、つまり支払カード21が充填端末11と共通の暗号鍵を有する正当な支払カードである認証し、受信したカードIDに対する処理を行う。

【0052】充填端末11は、受信したカードIDに基

づき、充填端末11の発行残高管理手段114が発行残高管理データベース13を参照して、支払カード21に対する充填限度額を取得する。これは、1枚の支払カード、つまり1カードIDに対する価値の発行額を制限するもので、発行額の制限が必要ない場合には取得する必要はない。

【0053】次に、充填端末11が支払カード21に対して充填限度額を通知するが、このときにも分離した乱数R3と充填限度額を合成して暗号化し、さらに発生した乱数R4とステータスS4を合成して送信し（ステップ504）、これを受信した支払カード21が充填端末11の認証を行うように、以下の通信では充填端末11と支払カード21はともに送信情報に分離した乱数を合成して暗号化し、さらに発生した乱数とステータスを合成して送信し、これを受信した側が認証を行うといった相互認証処理を通信毎に行うが認証方法は同様であるので以下では認証に関する説明は省略する。

【0054】さて、充填限度額の通知を受けた支払カード21は、その充填限度額の範囲内で価値の充填を受けるため、その充填額の減算要求を充填端末11に送信する（ステップ505）。減算要求を受けた充填端末11は、充填端末11の価値充填手段112に格納されている価値を減算するとともに同額の加算要求を支払カード21に対して送信し（ステップ506）、充填端末11の発行残高管理手段114が発行残高管理データベース13を更新する。

【0055】加算要求を受けた支払カード21は、支払カード21の価値加減算手段212が価値格納手段213に格納されている価値に、加算要求の額を加算することで価値を充填し、充填終了を充填端末11に通知する（ステップ507）。

【0056】なお、通信中に認証が失敗した場合やステータスの番号が不順となった場合には、通信に異常が生じたものとして充填処理を中止するが、充填処理では充填端末11側での減算処理の後に支払カード21の加算処理を行うため、発行した価値が不正に増額することはない。

【0057】図7（b）は、取引の際に支払カード21と取引端末32と収納カード31の間で授受されるデータの流れを示した図である。

【0058】まず、支払カード21と収納カード31が取引端末32に挿入され、支払カード21の送／受信手段214と取引端末32の送／受信手段321が接続され、収納カード31の送／受信手段314と取引端末32の送／受信手段322が接続されて支払カード21と取引端末32、収納カード31と取引端末32が通信可能な状態になると、販売者3が取引端末32の図示しない入力手段から取引する価値の額を入力する。

【0059】価値の額が入力されると、取引端末32の取引開始通知手段323が支払カード21に対して取引

開始要求を送信する（ステップ511）。なお、この取引開始要求には取引する価値の額が含まれている。

【0060】取引開始要求を受けた支払カード21は、収納カード31と通信を行って価値の移動を行うが、以下の通信には取引端末32は介入せずに支払カード21と収納カード31の間でのみ通信が行われる。また、支払カード21と収納カード31は、通信を行う際には、その通信毎に支払カード21の相互認証手段211と収納カード31の相互認証手段311の動作により相互に認証を行うが、その認証方法は上述の充填処理で説明したのと同様であるので、ここでは説明は省略する。

【0061】さて、取引開始要求を受けた支払カード21は、取引要求を収納カード31に送信する（ステップ512）。この取引要求には、取引する価値の額と支払カード21のカードID格納手段215に格納されている支払カード21に固有のカードIDが含まれている。

【0062】次に、収納カード31が取引額に応じた減算要求を支払カード21に対して送信し（ステップ513）、これを受けた支払カード21では、支払カード21の価値加減算手段212が価値格納手段213に格納されている価値を減算するとともに、減算額（取引額）に応じた加算要求を収納カード31に送信する（ステップ514）。

【0063】加算要求を受けた収納カード31では、収納カード31の価値加減算手段312が価値格納手段312に格納されている価値に、加算要求で要求された取引額を加算する。このとき、価値格納手段312は、格納する価値を先に取得したカードIDと対応させて格納する。

【0064】加算要求に対する処理が終了すると、収納カード31は取引終了を支払カード21に通知し、価値の移動（取引）処理を終了する（ステップ515）。

【0065】また、取引端末32は、支払カード21と収納カード31の通信に介入することはないが、その通信内容を傍受してステータスSnを取得することにより取引の進行状況を知ることができる。

【0066】図7（c）は、価値清算の際に収納カード31と清算端末12との間で授受されるデータの流れを示した図である。

【0067】まず、収納カード31が清算端末12に挿入され、収納カード31の送／受信手段314と清算端末12の送／受信手段123が接続されて収納カード31と清算端末12が通信可能な状態になると、収納カード31が清算する価値の額（通常は全額）を含んだ清算要求を清算端末12に送信する（ステップ521）。このとき、収納カード31は、暗号化した清算要求に収納カード31の相互認証手段311で発生した乱数R1とステータスS1を合成して送信するが、これは上述の価値充填の際に説明した相互認証と同様に、前記相互認証手段311と清算端末12の相互認証手段121が相互

認証を行うために使用するものであり、以下、通信毎に相互認証を行うがその認証方法は同様であるため、ここでは説明は省略する。

【0068】次に、清算要求を受けた清算端末12が収納カード31に対して、収納カード31が有する所有者IDを通知するようID通知要求を送信し（ステップ522）、これを受けた収納カード31が収納カード31の所有者ID格納手段315に格納されている収納カード31の所有者（販売者3）に固有の所有者IDを清算端末12に送信する（ステップ523）。

【0069】所有者IDを受けた清算端末12は、清算額に応じた減算要求を収納カード31に送信する（ステップ524）。

【0070】減算要求を受けた収納カード31では、収納カード31の価値加減算手段312が減算要求に応じて価値格納手段313に格納されている価値を減算するとともに、清算端末12に加算要求を送信する（ステップ525）。この加算要求には価値格納手段313に格納されていた（価値加減算手段312が減算した）価値に対応して記憶されていたカードID（価値発行時に発行先となった支払カードに固有のID）が含まれている。

【0071】加算要求を受けた清算端末12では、清算端末12の価値格納手段122に加算要求に応じた価値を格納（加算）するとともに、清算端末12の発行残高管理手段124が加算要求に含まれるカードIDとこれに対応した価値の額に基づいて発行残高管理データベース13の記憶内容を更新し、収納カード31に清算終了を通知して清算処理を終了する（ステップ526）。

【0072】以上、価値の充填、取引、清算の際の価値の移動を説明したが、ここで、価値の流れと不正行為の検出について説明する。

【0073】カード発行者1が発行する価値は、充填端末11から使用者2の所有する支払カード21に充填される。このとき、充填端末11は充填した価値の額と充填先の支払カード21のカードIDを対にして発行残高管理データベース13に記録する。また、一度充填を行った支払カード21にさらに価値を充填する際には、発行残高管理データベース13を参照して、支払カード21に対する価値の発行限度額の範囲内で充填を行い（発行限度額が設定されている場合のみ）、充填後は発行残高管理データベース13の記録を更新する。

【0074】使用者2が販売者3から商品またはサービスの提供を受けると、その対価として、支払カード21から取引端末32を介して収納カード31へ価値を移動する。

【0075】販売者3は、使用者2から受けとった価値を清算して現金化する際には、収納カード31に格納されている価値をカード発行者1の清算端末12へ移動させる。このとき、清算端末12は、収納カード31から

移動された価値の価値額とこれに対応したカードID番号に基づいて発行残高管理データベース13の記録を更新する。

【0076】価値の充填、取引、清算の各過程では、上述のように価値の送り側と受け側とで相互認証を行いながら、送り側での価値の減額の後に受け側での価値の増額を行って価値を移動させているため、支払カード21や収納カード31を偽造することは困難であり、価値の移動中にカードを引き抜くなどの操作を行っても、価値を増額することはできない。

【0077】また、仮にカードの偽造や価値の複製等が行われたとしても、カード発行者1は発行残高管理データベース13の記録に基づいて、不正行為を検出することができる。

【0078】図8は、不正行為の検出の流れを示すフローチャートである。発行残高管理データベース13が動作を開始し（ステップ601）、充填または清算による価値の額に対する更新処理があった場合に（ステップ602でYES）、その更新処理を行う価値と対応するカードIDに関する記録を検索し（ステップ603）、その記録（充填または清算価値額）を更新する（ステップ604）。

【0079】記録の更新の結果、充填した価値額よりも清算した価値額の方が大きくなった場合には（ステップ605でYES）、不正行為が行われたことを検出し（ステップ606）、不正検出処理を終了する（ステップ607）。

【0080】不正が検出された場合には、清算時に取得した収納カード31の所有者IDと価値と対応するカードIDに基づいて追跡を行う。

【0081】また、支払カード21と収納カード31の両者に価値の移動を行う毎に、その内容を履歴として記録するように構成しておけば、不正が生じた場合には、そのカードを不正の証拠とすることができる。

【0082】なお、支払カード21にカードIDを付さずに使用した場合にもセキュリティ上は所定の効果が得られ、カードIDを付した場合にもカードIDと使用者2の関係を登録する必要はないので使用者2のプライバシーを保つことは可能である。

【0083】次に、この発明に係わるICカードを用いた決済方法およびシステムの第2の実施例について説明する。

【0084】この第2の実施例では、カード発行者が発行する価値に発行番号（識別番号）を付して発行し、この発行番号を利用することで発行した価値の管理や不正の検出を行う。

【0085】この第2の実施例におけるシステムは、上述の第1の実施例と同様に、カード発行者1が有する充填端末11と清算端末12と発行残高管理データベース13、使用者2が有する支払カード21、販売者3が有

する収納カード31と取引端末32で構成される(図1参照)。

【0086】また、システムを構成する各部も上述の第1の実施例とほぼ同様であるので異なる点のみを説明する。

【0087】第2の実施例では、価値に付した発行番号を利用して発行した価値の管理や不正の検出を行うため、支払カード21が該カードに固有のカードIDを格納する必要がなく、支払カード21のカードID格納手段215を具備しない。また、充填端末11の価値充填手段112と発行残高管理手段114、清算端末12の価値格納手段122と発行残高管理手段124、支払カード21の価値格納手段212、収納カード31の価値格納手段312は、常に価値とその価値に付された発行番号を対応させて処理を行う。

【0088】つまり、充填端末11から発行された価値には必ず発行番号が付され、この発行番号は同一の時間に同一の支払カード21へ発行する価値は同一の番号となるが、異なる時間や異なる支払カード21に対して発行する価値には異なる発行番号となる。支払カード21は、取引により収納カード31に価値を移動する際には、価値とその価値の発行番号を対にして移動させる。このとき、取引により移動する価値の額が、充填端末11より発行を受けた額よりも小さい場合には、価値が分割されるため、同一の発行番号を持つ価値が存在することになる。

【0089】したがって、発行残高管理データベース13は、清算された価値を発行番号毎に累積し、清算額が発行額を越えた価値が検出された場合にはそれを不正検出とする。

【0090】なお、この第2の実施例においても価値の移動の際には、第1の実施例と同様に価値の送り側と受け側が相互に認証を行う。

【0091】次に、この発明に係わるICカードを用いた決済方法およびシステムの第3の実施例について説明する。

【0092】この第3の実施例は、上述の第1の実施例および第2の実施例における支払カード21と収納カード31の両者を収支カードとして1枚のICカードに具備したカードを利用する。

【0093】図9は、収支カードの構成を示すブロック図である。収支カード41は、相互認証手段411、価値加減算手段412、価値格納手段413、送/受信手段414、所有者ID格納手段415、カードID格納手段416を具備して構成される。相互認証手段411は、送/受信手段414を介して接続される充填端末11や清算端末12、支払カード21、収納カード31、他の収支カード41とその正当性を相互に認証する手段であり、価値加減算手段412は、相互認証手段411により認証された相手との価値の移動のために価値格納

手段413に格納されている価値の加算および減算を行う。

【0094】この収支カード41は、上述の各実施例における支払カード21と収納カード31の両者として使用でき、その動作は上述の実施例と同様なので説明は省略する。

【0095】なお、収支カード41が具備するカードID格納手段416は、上述の第2の実施例に対応させる場合には具備する必要はない。

10 【0096】また、上述の各実施例で説明したように、支払カード21(または収支カード41)から収納カード31(または収支カード41)へ価値を移動させる際に、取引端末32は両者の通信に介入しない。つまり、取引端末32は各実施例における決済システムのセキュリティには関与していない。

【0097】したがって、支払カード21(または収支カード41)から収納カード31(または収支カード41)への価値の移動は、通信回線を介して行うこともできる。この通信回線は専用線や電話回線等の比較的セキュリティ性の高いものでも、インターネットのようにセキュリティ性の低いものでも利用できる。

【0098】例えば、図10(a)に示すように、インターネット50に接続された端末51-1乃至51-6のいずれかの間で価値の移動を行うことができ、インターネット上でのオンラインショッピングの決済に利用することもできる。この場合の各端末51-1乃至51-6は、専用の端末でもパーソナル・コンピュータ等にICカードリーダー/ライタを接続してこれを端末として利用してもよい。

30 【0099】また、図10(b)に示すように、収納カード31(または収支カード41)を挿入する端末60に、支払カード21(または収支カード41)を挿入する複数の端末61-1乃至61-4を接続して価値の移動を行うことができる。この図10(b)に示すシステムは、例えば商店等において、端末60を事務室に設置して端末61-1乃至61-4を夫々レジスタに配置することで売り上げの全てを1枚の収納カードに集約する場合等に利用できる。

【0100】なお、上述の各実施例において、充填端末11に現金収受機能や、口座引落機能、クレジット決済機能等を設け、清算端末12に現金払出機能や口座振込機能等を設けることでより一層、利用範囲を広げることができる。

【0101】

【発明の効果】以上説明したように、この発明によれば、使用者が身分を明かすことなく支払カードへの価値の充填および販売者との取引を行い、販売者は身分を明かして価値の清算を行い、支払カードと収納カードが相互認証を行って価値を移動させるように構成したので、使用者のプライバシーが保護できるとともに支払カード

の譲渡が可能となり、価値を移動させる際の取引端末はシステムの安全に関与しないため、通信を介したり広範囲に設置したりすることができる。また、偽造価値の使用等の不正に加え販売者の脱税等の不正を行うことも困難とすることができる。

【0102】また、支払カードに固有のIDや発行価値に固有の発行番号等を利用することで不正が生じた場合の追跡を容易に行うことができる。

【図面の簡単な説明】

【図1】ICカードを用いた決済システムのシステム構成を示すブロック図。

【図2】充填端末の詳細を示すブロック図。

【図3】清算端末の詳細を示すブロック図。

【図4】支払カードの詳細を示すブロック図。

【図5】収納カードの詳細を示すブロック図。

【図6】取引端末の詳細を示すブロック図。

【図7】価値の充填、取引、清算の際の各々の通信データの流れを示した図。

【図8】不正行為の検出の流れを示すフローチャート。

【図9】収支カードの構成を示すブロック図。

【図10】決済システムの利用例を示した図。

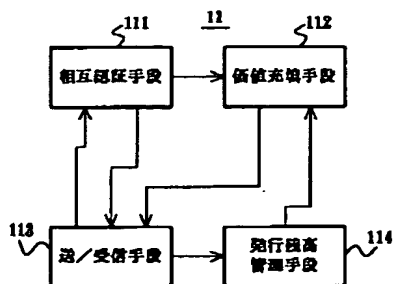
【図11】従来のシステムにおける流通過程でのICカード内に格納されている価値の形態を示した図。

【符号の説明】

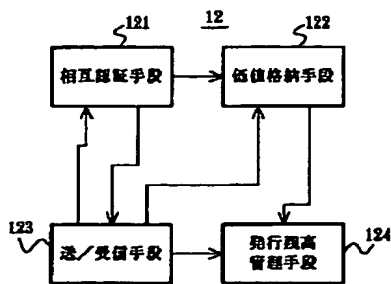
- 1 カード発行者
- 2 使用者
- 3 販売者
- 11 充填端末
- 12 清算端末
- 13 発行残高管理データベース
- 21 支払カード
- 31 収納カード
- 32 取引端末

- 41 収支カード
- 50 インターネット
- 51-1～51-6 端末
- 60 端末
- 61-1～61-4 端末
- 111 相互認証手段
- 112 価値充填手段
- 113 送/受信手段
- 114 発行残高管理手段
- 121 相互認証手段
- 122 価値格納手段
- 123 送/受信手段
- 124 発行残高管理手段
- 211 相互認証手段
- 212 価値加減算手段
- 213 価値格納手段
- 214 送/受信手段
- 215 カードID格納手段
- 311 相互認証手段
- 312 価値加減算手段
- 313 価値格納手段
- 314 送/受信手段
- 315 所有者ID格納手段
- 321 送/受信手段
- 322 送/受信手段
- 323 取引開始通知手段
- 411 相互認証手段
- 412 価値加減算手段
- 413 価値格納手段
- 414 送/受信手段
- 415 所有者ID格納手段
- 416 カードID格納手段

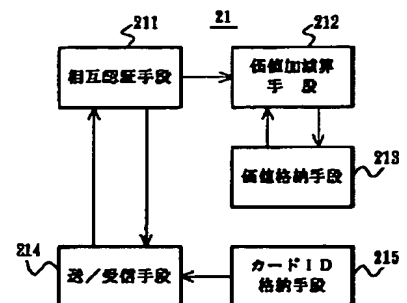
【図2】



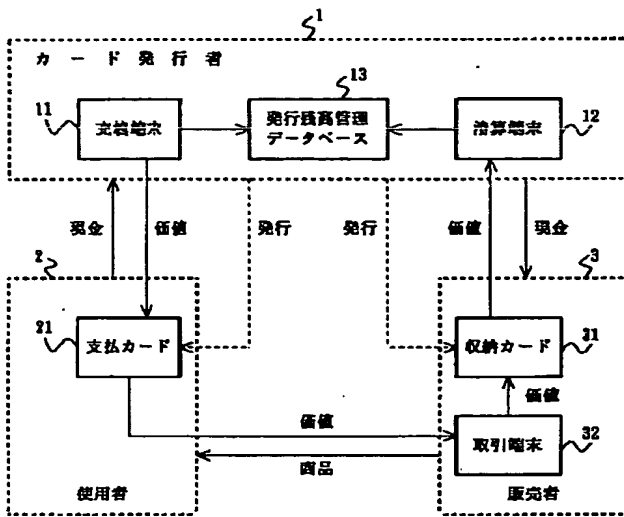
【図3】



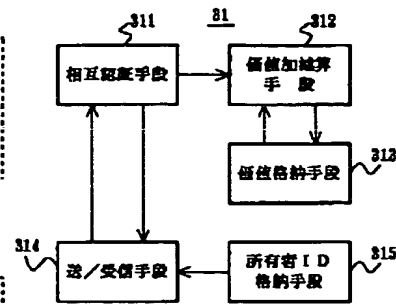
【図4】



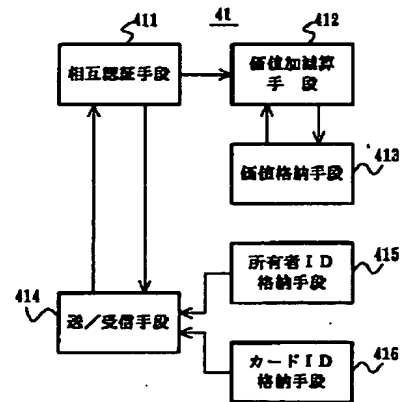
【図1】



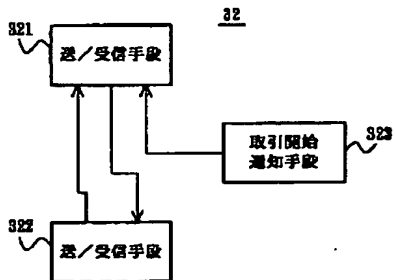
【図5】



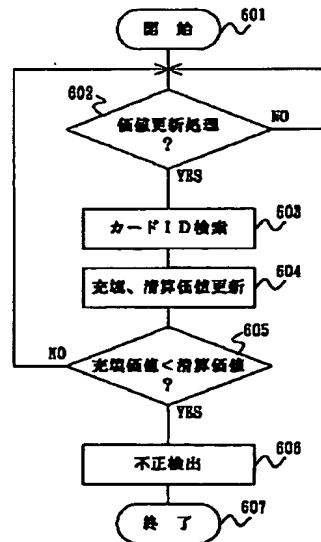
【図9】



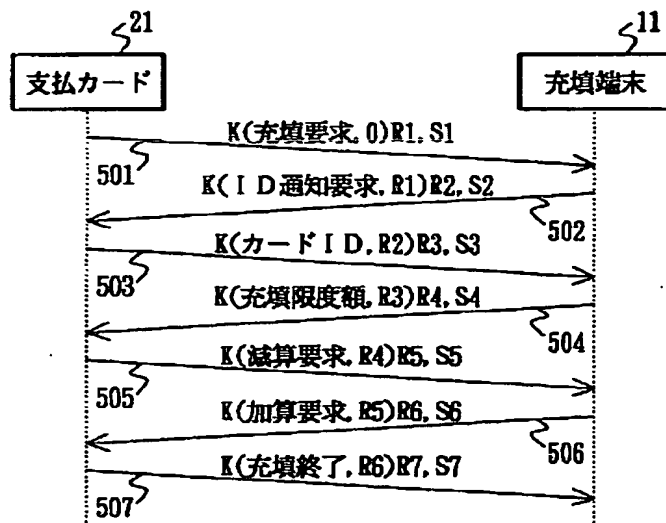
【図6】



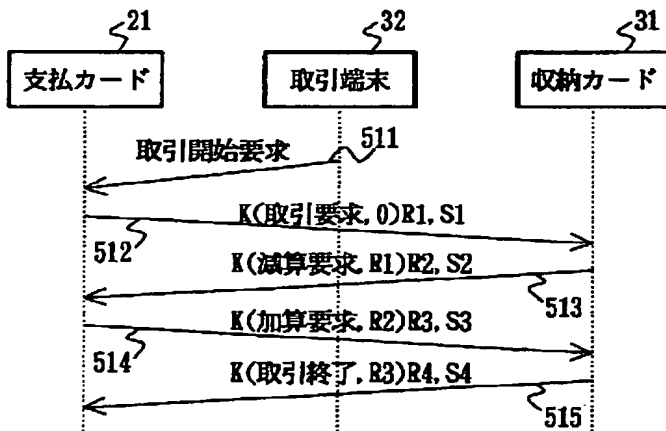
【図8】



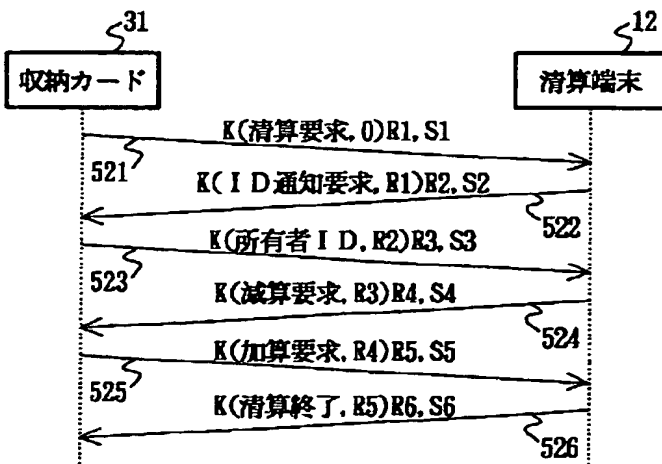
【図 7】



(a)

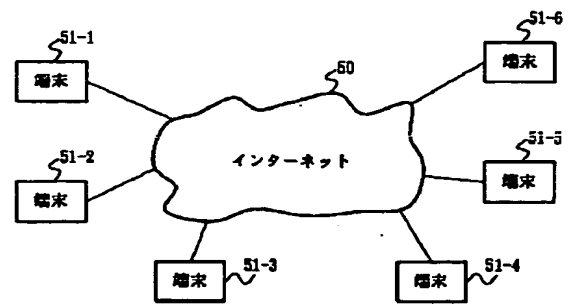


(b)

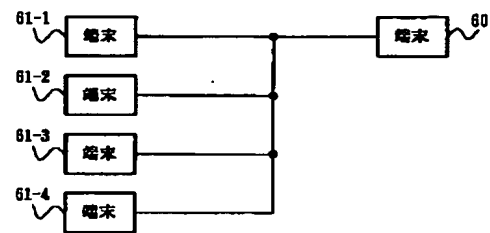


(c)

【図 10】

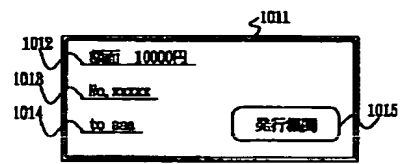


(a)

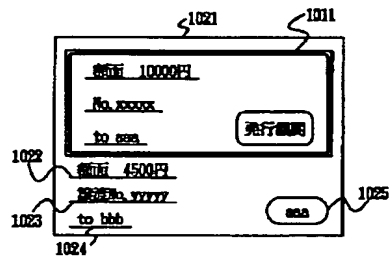


(b)

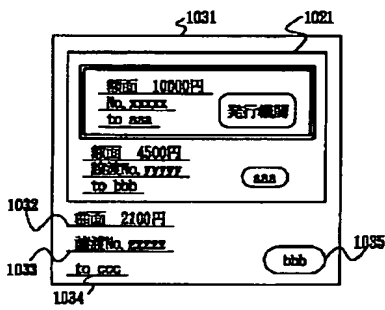
【図 1 1】



(a)



(b)



(c)

フロントページの続き

(51) Int. Cl. ⁶

G 0 7 G 1/12
1/14

識別記号
3 2 1

F I

G 0 6 K 19/00
G 0 7 F 7/08

R
Z